

常见问答 FAQ

一、关于卡的 FAQ:

1、问：M1 卡的密码 A 和密码 B 有什么区别？

答：一般来讲国内新卡片（空白卡）中的控制字（FF 07 80 69）密码 A 可用，密码 B 不可用；密码有效时是不能读的，只能写，读出来的一律以全 0 填充，白卡默认的控制位数据为 FF078069，这时 KeyB 可以读，就不能作为密码使用。

如果想使用 KeyB，请更改控制位为 7F078869，使 KeyB 不可以读，这样就可以用 KeyB 了。这是 M1 卡的规则，具体请查阅 NXP 原版 m1 卡的英文资料，上面有说明

推荐的控制字

方案一：7F 07 88 69

此控制字说明：数据块：用密码 A 或 B 都可以读写；

控制块：密码 A：由密码 B 来写，不可读；

密码 B：由密码 B 来写，不可读；

控制字：用密码 A 或 B 都可读，由密码 B 写；

方案二：08 77 8F 69

此控制字说明：数据块：用密码 A 读，由密码 B 读写；

控制块：密码 A：由密码 B 来写，不可读；

密码 B：由密码 B 来写，不可读；

控制字：用密码 A 或 B 都可读，由密码 B 写；

2、mifare卡的状态有哪些？

答：有下面几种状态：

(1)、POWER OFF （断电状态）

卡片由于缺少射频磁场能量而处于断电状态卡片不工作。

(2)、IDLE （休眠状态）

卡片被电磁场能量激活后延迟数毫秒则进入IDLE 状态，在这一状态中能够解调读卡器传来的调制信号并能对读卡器的Request 以IDLE 或ALL 方式命令进行应答。

(3)、READY （就绪状态）

当对Request 命令进行应答后就进入了READY 状态,在这一状态中可以采用比特帧防冲突算法,当卡片的唯一序列号被读卡器发来的Selection 命令选中时就退出本状态。

(4)、ACTIVE （激活状态）

当卡片的唯一序列号被读卡器选中时就进入本状态, 在这一状态中卡片完成本次应用所要求的全部操作。

(5) HALT 停止状态

卡片应用完成后,读卡器可通过发送Halt 命令,使卡片进入这一状态,在这一状态中卡片只对读卡器以ALL 方式发送的Request命令进行应答(或被唤醒),从而又进入READY 状态。

3、值块（value）的格式？

值块在卡中可以实现电子钱包的功能,它有一个固定的格式,可以进行错误检测和纠正,在对其进行操作时需要按照这种格式来进行。

值块的这种标准格式只能在格式化值块的写操作时产生:

- 1)、Value: 表示一个带符号4 字节值,这个值的最低一个字节保存在最低的地址中,取反的字节以标准2的格式保存,为了保证数据的正确性和保密性,值被保存了3次,两次不取反保存一次取反保存,
- 2)、Adr : 表示一个字节地址,当执行强大的备份管理时用于保存存储段的地址,地址字节保存了4 次,取反和不取反各保存两次。在执行增减恢复传送操作时地址保持不变,它只能通过写命令改变。

Byte Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	Value				Value				Value				Adr	Adr	Adr	Adr

4、值块操作

问:

在对数据块进行值操作时参数*_Value 需要减的值应该是十进制还是十六进制
是低位在前还是高位在前,例如我要减1000 ,*_Value 指向的值应该是00 00 10 00 或00 10 00 00 还是应该是E8 03 00 00 或 00 00 03 E8 为什么?

答:

这实际上是高级语言和机器语言的转换问题,在对参数*_Value进行赋值时若要减1000,十进制可以是1000 或0x3E8 那么在C51 编译器编译后在内存中它的存储方式是00 00 03 E8

其高位在低地址而低位却在高地址而卡中这个数的存放顺序为E8 03 00 00两者正好位置颠倒。

5、S50 和 S70 卡的区别？

s50 卡有 1k bytes（1 字节等于 8 比特）

共 16 个扇区，每个扇区有 4 个块，其中第 0 扇区的第 0 块是卡序列号，是只读的，不能写。密码存放在每个扇区的块 3。

算存储密码块的算法是： $x=s*4+3$ ；其中 s 表示扇区号（0—15）。

s70 卡有 4k bytes

共 40 个扇区

分两部分：第一部分为 32 个扇区

第二部分为 8 个扇区

前 32 个（0—31）扇区每个区有 4 个块，每个块有 16 个字节，密码在每个区的块 3。

算存储密码块的算法是： $x=s*4+3$ ；其中 s 表示扇区号（0—31）。

后 8 个（32—39）扇区每个扇区有 16 个块，每个块有 16 个字节，密码在每个区的块 15。

算存储密码块的算法是： $x=128+s*16+15$ ；其中 s 表示后 8 个扇区号（0—7）。

所以后 8 个扇区适合作为信息存储区，可以一次存储大量的信息。

6，如何修改 M1 卡密码？

答：修改密码其实和写数据块是一样的操作，不同的是密码放在每个扇区的最后一个块，关于密码块的算法请参考问题 5。

密码块由密码 A(6 个字节) + 控制字(4 个字节) + 密码 B(6 个字节) 共 16 个字节组成。

一般 M1 的出厂密码不管是 A 还是 B 都是 12 个 F，也就是说，初始化的密码块 16 个字节内容是：

FFFFFFFFFFFF FF078069 FFFFFFFFFFFFFF（为了区分特意加了空格，实际没有空格）

一般以应用 A 密码的多，B 密码出厂时有的没有激活的。注意，有效的密码是读不出来的，读的时候全以 0 填充。

现在先假设要修改扇区 02 的 A 密钥为 112233445566，那么可以执行下面的操作（密码块 $=2*4+3=11$ ）：

YHY502 的写指令代码是 0x22，

命令是这样的（16 进制）：

1A 22 00 0B FF FF FF FF FF FF 11 22 33 44 55 66 FF 07 80 69 FF FF FF FF FF FF 55

另外，YHY502C 新增了 [Change_Card_Keys 密码修改](#) 指令 0x06，省去开发人员算扇区的麻烦，具体请参考 [YHY502C 新增指令的补充说明](#)。

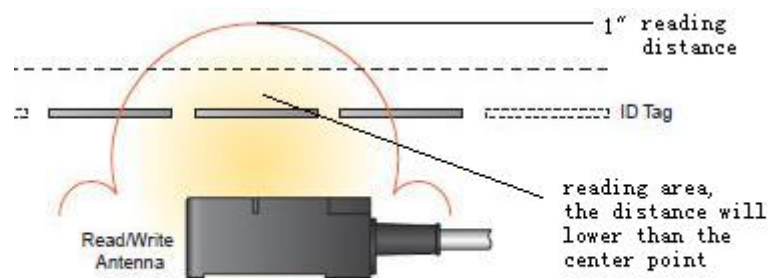
二、关于读写器的 FAQ

1、问：内置天线和外置天线有什么区别？

答：内置天线是和读卡基站做在同一个 PCB 上，外置天线则是天线和读卡基站分离。

2、问：天线的正面和反面有区别吗？

答：基本没有区别，通信的能量主要集中在天线的中心区域，天线外延信号会减弱很快。



3、问：若多个射频模块安装在一块，实际要求一块卡片对应一个模块，那么他们之间是否会互相干扰。（这个对应的现场应用是，因为电力公司安装电能表，会集中在一个表箱里面，那么在表箱里面有多个“射频读写的电能表”的情况下，如何能保证单个用户只操作自己的电能表，而其他电能表不会产生干扰或误操作。）

答：模块在电表工程实际安装之间的距离不会互相干扰，至于如何保证单个用户只操作自己的电能表可以通过对应的 ID 号和权限属性来设置，RFID 技术在这方面可以做得很好，RFID 具有防冲突功能，能有效识别不同的卡，不会产生误操作。

4、问：为保证通讯效果，对外围安装介质的有什么要求？（也就是说射频非接触式电能表建议安装在什么类型的表箱里面，非金属的还是金属的或其它？）

答：由于射频信号容易受到金属环境和介质的影响，所以，在天线的表面以不能是大面积的金属，天线的边沿以及底部距离金属需要有 1cm 左右以上的距离。在金属环境下天线的特性以及读取距离会受影响。特殊情况可以根据电表箱来设计天线。电表箱的其它部分可以是金属的。

5、YHY502 模块的 RST 复位脚怎么接？

答：这个 RST 管脚可以不接，上电模块会自动复位，如果要连接不要和控制器的复位脚并接，可以接到控制器的其中一个 IO 管脚，要复位模块时可以发送一个低电平脉冲就可以使之复位。

6、YHY502C 能直接和 PC 连接通信吗？

答：不能。

YHY502C 是通过 UART 和主机通信的，如果要和 PC 直接通信，那么可以通过一个 MAX232（如果是 3.3V 工作的则用 MAX3232）作为电平转换后再接到 PC，同时必须给模块供 5V 或者 3.3V 电压。另一种办法就是通过 232 转 USB 的电路比如 CP2102 之类的进行连接。

